UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/672,602	09/29/2000	Carl M. Ellison	042390.P8629X	2068

7590 01/11/2005

Thinh V Nguyen
Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard
7th Floor
Los Angeles, CA 90025

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/672,602	ELLISON ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cov r sheet with the correspond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-80* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on July 27, 2004. Claims 1 – 80 were originally received for consideration. Claims 1- 3, 17- 19, 21 -23, 37 - 39, 41 - 43, 46 - 55, 57 - 59, 61- 63,78, and 79 are currently amended. No claims were added or cancelled. Currently claims 1 – 80 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-5, 20-25, 40-45, 60-65, and 80 are rejected under 35 U.S.C. 102(e) as being anticipated by England et al. (U.S. Patent 6,327,652).

Regarding claim 1, England discloses:

An apparatus comprising:

a digest memory to store an isolated digest in a secure environment for an isolated execution mode, the secure environment being associated with an isolated memory area accessible by at least one processor, the at least one processor operating in one of a normal execution mode and the isolated execution mode (column 16 lines 50 – 67, column 12 lines 53 - 65); and

an attestation key memory (AKM) device coupled to the digest memory to attest the isolated execution mode and prove validity of a program loaded into the isolated memory area using the isolated digest (column 8 line 56 – column 9 line 51, column 11 lines 46 – 62, column 12 lines 53 – 65).

The "isolated execution mode" disclosed in the above claim, is interpreted as a mode in which other applications or other unauthorized areas of memory cannot access. England discloses a segment of memory (DRMOS) that prohibits the use of certain programs, prevents tampering, provides a secure storage space, and can prohibit all access when a trusted application is running (executing) (column 15 line 62 – column 16 line 67). The function of preventing access to a memory while a certain application is running can be interpreted as "isolated execution mode" because access is prohibited while the trusted application is running in the DRMOS. The DRMOS has an isolated secure key storage area. The keys (digests) are stored are used to validate components (programs) before they are loaded into the DRMOS (isolated memory area) and a cryptographic hash of all the components that are loaded into the DRMOS is made (column 12 lines 53 – 65) and are stored in an internal register in the CPU.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, England discloses:

The apparatus of claim 1 wherein the isolated digest includes at least a digest of one of a processor nub loader, a processor nub, an operating system nub, and a supervisory module loaded into an isolated execution space (column 9 lines 1 – 10, column 16 lines 50 – 67, column 12 lines 53 - 65).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, England discloses:

The apparatus of claim 2 further comprising:

an interface to map the device to an address space of a chipset in the secure environment (column 13 line 60 – column 14 line 23); and

a communication storage corresponding to the address space to allow the AKM device to exchange security information with the at least one processor, the security information including at least one of a static public key and a static key certificate (column 5 lines 1 – 51, column 11 line 46 – column 12 line 36).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, England discloses:

The apparatus of claim 3 wherein the device accesses a chipset storage via the address space (column 5 lines 1 – 51, column 11 line 46 – column 12 line 36).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, England discloses:

The apparatus of claim 4 wherein the communication storage comprises:

a configuration storage to store device configuration information (column 5 lines 1 – 51, column 11 line 46 – column 12 line 36).

Claim 20 is rejected as applied above in rejecting claim 3. Furthermore, England discloses:

The apparatus of claim 3 wherein the device accesses a remote server via the address space (column 6 lines 55 – 67, column 9 line 30 – column 10 line 40).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 6-19, 26-39, 46-59, and 66-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over England et al. (U.S. Patent 6,327,652) in view of Ermolovich (U.S. Patent 4,319,323).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, England discloses the communication storage as applied to claim 5. England does not explicitly disclose:

"a status register to store device status of the device;

a command register to store a device command for a command interface set; and

an input/output block(IOB) to store input and output data corresponding to the command".

However, Ermolovich discloses a status register to store device status (see col. 85, lines 37-45), a command register to store a device command (see col. 12, lines 2-6) and an input/output block to store input and output data (see col. 71, lines 40-64). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine England's system of ensuring integrity throughout post processing with the teaching of Ermolovich's communication device with data processing system by including the status register, the command register and the input/output block taught by Ermolovich to prevent data from being lost or corrupted during data transfers between a data processing system and an external device (see Ermolovich et al. abstract and col. 3, lines 26-50).

Claim 7 is rejected as applied above in rejecting claim 6. Furthermore, England discloses:

The apparatus of claim 6 wherein the configuration storage comprises:

a public key storage to store the static public key (column 5 lines 1 – 51, column 11 line 46 – column 12 line 36);

a key certificate storage to store the static key certificate (column 5 lines 1 – 51, column 11 line 46 – column 12 line 36); and

an interface set storage to store an interface set identifier, the interface set identifier identifying a command interface set supported by the device (column 5 lines 1 – 51, column 11 line 46 – column 12 line 36).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, England discloses:

The apparatus of claim 7 wherein the configuration storage further comprises:

a manufacturer identifier storage to store a manufacturer identifier (column 7 line 45 – column 8 line 37); and

a revision storage to store a revision identifier (column 13 line 60 – column 14 line 57).

Clam 9 is rejected as applied above in rejecting claim 7. England does not explicitly discloses the command interface set containing an initialization set, the initialization set supporting a reset command and a connect command. Ermolovich discloses "wherein the command interface set is an initialization set, the initialization set supporting a reset command and a connect command" (column 54, lines 20 – 28). Furthermore, it would have been obvious to contain the reset and connect commands in the command

interface set because the command and reset commands are necessary for a host to initiate and then re-establish communications with a remote server.

Claim 10 is rejected as applied above in rejecting claim 7. Furthermore, England discloses:

The apparatus of claim 7 wherein the command interface set is an attestation set, the attestation set performing at least one of public key enumeration, a key certificate enumeration, and a signing operation (column 5 lines 1 – 51, column 11 line 46 – column 12 line 36).

Claim 11 is rejected as applied above in rejecting claim 10. England does not explicitly disclose:

The apparatus of claim 10 wherein the status register comprises a connection field to provide a connection status to indicate that the device is responsive to the connect command and an estimate field to provide an estimate of processing time for an operation specified in the command. Ermolovich discloses a connection field to provide a connection status to indicate that the device is responsive to the connect command (column 9 lines 7 – 17) and an estimate field to provide an estimate of processing time for an operation specified in the command (column 16 lines 1 – 14). Following the same logic used in rejecting the claims above, it is obvious that a connection status and an estimate processing time are well-known in the operation of connecting to a remote host. The connection status would provide a notification if the

connection is complete and the estimated processing time would map each operation to a time period to complete the operation.

Claim 12 is rejected as applied above in rejecting claim 11. England does not explicitly disclose the status register containing a self-test field to indicate status of a self-test in response to the reset command. Ermolovich discloses a self-test field to indicate status of a self-test in response to the reset command (column 86 lines 4 – 21). Following the same logic used in rejecting the claims above, it is obvious that a self-test field is well-known in the operation of connecting to a remote host. The self-test status would provide a notification if the reset command was successful or not, and therefore, is necessary to ensure that a connection is completed.

Claim 13 is rejected as applied above in rejecting claim 10. Furthermore, England discloses:

The apparatus of claim 10 wherein the public key enumeration enumerates an additional public key other than the static public key (column 13 line 54 – column 14 line 67).

Claim 14 is rejected as applied above in rejecting claim 10. Furthermore, England discloses:

The apparatus of claim 10 wherein the key certificate enumeration enumerates an additional key certificate other than the static key certificate (column 9 line 42 – column 10 line 52).

Claim 15 is rejected as applied above in rejecting claim 10. Furthermore, England discloses:

The apparatus of claim 10 wherein the sign operation generates a signature to attest validity of the secure environment using a private key provided by the chipset (column 8 line 56 – column 9 line 51, column 11 lines 46 – 62, column 12 lines 53 – 65).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, England discloses:

The apparatus of claim 15 wherein the signature corresponds to signing a chipset parameter (column 8 line 56 – column 9 line 51, column 11 lines 46 – 62, column 12 lines 53 – 65).

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, England discloses:

The apparatus of claim 16 wherein the chipset parameter is one of a processor nub loader hash, a chipset hash log, a software hash, and a nonce (column 8 line 56 – column 9 line 51, column 11 lines 46 – 62, column 12 lines 53 – 65).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, England discloses:

The apparatus of claim 17 wherein the processor nub loader hash and the chipset hash log are stored in the chipset storage (column 16 lines 50 – 67, column 12 lines 53 - 65).

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, England discloses:

The apparatus of claim 18 wherein the software hash and the nonce are provided by a processor nub (column 8 line 56 – column 9 line 51, column 11 lines 46 – 62, column 12 lines 53 – 65).

4. Claims 21 – 40 are method claims analogous to the apparatus claims 1 – 20 rejected above, and are therefore rejected following the same reasoning.

5. Claims 41-60 are computer program product claims analogous to the apparatus claims 1 – 20 rejected above, and are therefore rejected following the same reasoning.

6. Claims 61-80 are system claims analogous to the apparatus claims 1 – 20 rejected above, and are therefore rejected following the same reasoning.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3796. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
01/06/05

E. Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER